

CLAIMS

What is claimed is:

1. A method for migrating a base chip key from a first computer system to a second computer system, wherein said first computer system includes a base chip key 1, and said second computer system includes a base chip key 2, said method comprising:

generating a second certificate for said base chip key 1 by a manufacturer of said second computer system using a first certificate for said base chip key 1, and generating a second certificate for said base chip key 2 by a manufacturer of said first computer system using a first certificate for said base chip key 2;

sending a first data packet from said first computer system to said second computer system, wherein said first data packet includes all data necessary to reproduce said base chip key 1 in said second computer system;

sending a second data packet from said second computer system to said first computer system acknowledging the receipt of a copy of said base chip key 1;

erasing said base chip key 1 from said first computer system; and

replacing said base chip key 2 in said second computer system with said base chip key 1.

1 2. The method of Claim 1, wherein said first data packet includes a first random
2 number.

1 3. The method of Claim 1, wherein said first data packet is encrypted with said base
2 chip key 1's public key.

1 4. The method of Claim 1, wherein said second data packet includes said first random
2 number and a second random number.

1 5. The method of Claim 1, wherein said second data packet is signed by said base chip
2 key 2.

1 6. The method of Claim 1, wherein said method further includes:

2 generating an identity key 1 in said first computer system, and generating
3 an identity key 2 in said second computer system;

4 generating a certificate for said identity key 1, and generating a certificate
5 for said identity key 2; and

6 generating a first certificate for said base chip key 1 using said identity key
7 1, and generating a first certificate for said base chip key 2 using said identity key
8 2.

1 7. A computer program product residing on a computer usable medium for migrating
2 a base chip key from a first computer system to a second computer system, said computer
3 program product comprising:

4 program code means for generating a second certificate for said base chip
5 key 1 by a manufacturer of said second computer system using a first certificate for
6 said base chip key 1, and generating a second certificate for said base chip key 2
7 by a manufacturer of said first computer system using a first certificate for said base
8 chip key 2;

9 program code means for sending a first data packet from said first computer
10 system to said second computer system, wherein said first data packet includes all
11 data necessary to reproduce said base chip key 1 in said second computer system;

12 program code means for sending a second data packet from said second
13 computer system to said first computer system acknowledging the receipt of a copy
14 of said base chip key 1;

15 program code means for erasing said base chip key 1 from said first
16 computer system; and

17 program code means for replacing said base chip key 2 in said second
18 computer system with said base chip key 1.

1 8. The computer program product of Claim 1, wherein said first data packet includes
2 a first random number.

1 9. The computer program product of Claim 1, wherein said first data packet is
2 encrypted with said base chip key 1's public key.

1 10. The computer program product of Claim 1, wherein said second data packet includes
2 said first random number and a second random number.

1 11. The computer program product of Claim 1, wherein said second data packet is
2 signed by said base chip key 2.

1 12. The computer program product of Claim 1, wherein said computer program product
2 further includes:

3 program code means for generating an identity key 1 in said first computer
4 system, and generating an identity key 2 in said second computer system;

5 program code means for generating a certificate for said identity key 1, and
6 generating a certificate for said identity key 2; and

7 program code means for generating a first certificate for said base chip key
8 1 using said identity key 1, and generating a first certificate for said base chip key
9 2 using said identity key 2.